

Wave Health Service Definition

1. Service Overview

1.1 About Wave Health

Wave Health is an Electronic Patient-Reported Outcomes (ePRO) platform that enables healthcare organisations to monitor patients remotely, capture patient-reported outcomes, and identify clinical issues early. The platform is registered as a Software as a Medical Device (SaMD) with UKCA Class I certification.

By replacing manual check-ins, phone calls, and ad-hoc follow-ups with structured digital symptom tracking and validated questionnaires, Wave Health allows clinical teams to focus on patients who truly need intervention.

1.2 Problems Addressed

- Clinical teams spend significant time on routine monitoring and follow-up activities
- Patients are often unseen between appointments
- Important symptom changes are missed or identified too late
- Manual processes create capacity burdens on nursing staff

Wave Health automates routine monitoring and flags risk, reducing unnecessary contact and avoiding avoidable clinical escalation.

1.3 Core Capabilities

Capability	Description
Digital Symptom Tracking	Structured well-being check-ins and symptom reporting from patients
ePRO Questionnaire Delivery	Validated or custom patient-reported outcome measures
Early Risk Identification	Automated prioritisation and alerting for clinical review
Research Data Collection	High-quality longitudinal data capture for real-world evidence

1.4 User Types

User	Role
Patients	Report symptoms and complete questionnaires from home
Nurses & Clinicians	Review dashboards, prioritise patients requiring attention
Researchers	Collect and analyse longitudinal outcome data
Administrators	Manage patient populations, users, and configurations

2. Data Backup and Recovery

2.1 Backup Schedule

Backup Type	Frequency	Description
Differential	Monday – Thursday	Captures changes since the last full backup
Full	Every Friday	Complete backup of all data
Monthly	Last Friday of each month	Long-term retention backup

Point-in-Time Recovery (PITR) is enabled for all production databases, allowing restoration to any point within the retention window.

2.2 Backup Scope

The following data is included in backup processes:

- Relational database systems (RDS) containing patient and operational data
- Object storage (S3) containing protected health information
- Application configuration data

2.3 Retention Period

All backup data containing protected health information is retained for **7 years** in accordance with HIPAA regulatory requirements.

2.4 Geographic Considerations

Backup data remains within the same geographic region as the source production environment to comply with data residency requirements. Backups are not replicated across regional boundaries.

2.5 Recovery Objectives

Metric	Target	Description
Recovery Point Objective (RPO)	1 hour	Maximum acceptable data loss in the event of a failure
Recovery Time Objective (RTO)	4 hours	Target time to restore full service following a major incident

2.6 Backup Testing

Backup restoration procedures are tested at least **annually** to verify data integrity and recovery processes.

3. Disaster Recovery and Business Continuity

3.1 Scope

The disaster recovery plan addresses the following scenarios:

- Full regional infrastructure outage
- Database corruption
- Ransomware or malicious data destruction

3.2 Recovery Approach

Wave Health operates a single-region deployment model per jurisdiction with manual failover capabilities. This architecture balances cost efficiency with regulatory compliance for data residency.

Component	Approach
Database Recovery	Manual failover using Point-in-Time Recovery
Application Recovery	Redeployment from infrastructure-as-code templates
Region-Level Outage	Manual recovery procedures; data residency constraints limit cross-region replication

3.3 Business Continuity Testing

Disaster recovery procedures are tested at least **annually** through tabletop exercises and technical recovery drills.

3.4 Incident Communication

Customer communication during major incidents follows the Incident Response Plan. Initial notification is provided within 4 hours of incident identification via email to designated customer contacts.

4. Onboarding Support

4.1 Onboarding Process

Wave Health provides a guided, turnkey onboarding process that includes:

- **A dedicated implementation team** is assigned to each deployment
- **Clinical workflow approval** – confirmation of clinical guidelines, workflows, and responsibilities
- **Platform configuration** using Wave Health's standard, production-ready framework
- **Mandatory user training** (~2 hours) required prior to system access
- **Go-live support**, including early-stage quality assurance and weekly feedback sessions during the first month

4.2 Timeline

Onboarding is typically completed within **30 days**, with most deployments going live in **2–4 weeks**, subject to:

- Clinical approvals
- IT access enablement
- Training completion

4.3 Customer Responsibilities

Customers are required to provide:

Requirement	Description
Project Leadership	Named clinical and project leads
Workflow Approval	Sign off on clinical guidelines and workflows
User Management	User lists and role assignments
Training Completion	All users must complete mandatory training
IT Enablement	Domain/IP whitelisting as required
Governance	Appropriate data governance and information governance approvals

5. Offboarding and Data Exit

5.1 Data Export

Upon contract termination or customer request, Wave Health can provide data export through a managed process. Export requests should be submitted to the designated account contact.

Current format: Database export (structured data)

Planned enhancement: Self-service export functionality

5.2 Data Retention Post-Termination

Customer data is retained for **7 years** following contract termination in accordance with healthcare regulatory requirements (HIPAA).

5.3 Data Deletion

Upon request, and after the retention period, data is deleted using cryptographic erasure methods. A formal Data Deletion Certificate is available upon request, confirming:

- Date of deletion
- Scope of data deleted
- Method of destruction
- Confirmation of completion

5.4 Transition Support

Customers may request data exports during the transition period before deletion. Export requests should be submitted with reasonable advance notice to allow for processing.

6. Service Constraints

6.1 Scheduled Maintenance

Parameter	Detail
Maintenance Window	Friday, midnight (UTC)
Advance Notice	Minimum 1 week
Rationale	Scheduled during the lowest-usage period to minimise clinical impact

6.2 Emergency Maintenance

Security vulnerabilities and critical patches are deployed immediately as required. Wave Health uses a blue-green deployment architecture enabling zero-downtime deployments for most releases.

6.3 Platform Standardisation

Wave Health operates as a standardised platform. Customer-specific customisations are not supported. This approach ensures:

- Consistent security controls across all deployments
- Validated clinical workflows meeting regulatory requirements
- Predictable system behaviour and performance
- Simplified compliance and audit processes

6.4 Usage

There are no predefined limits on:

- Number of patients
- Number of users
- Data storage
- API requests

Fair and reasonable use is expected in accordance with the service agreement.

7. Service Levels

7.1 Availability

Metric	Target
Platform Availability	99.9% monthly uptime
Measurement Period	Calendar month
Exclusions	Scheduled maintenance windows

99.9% availability equates to approximately 43 minutes of unplanned downtime per month.

7.2 Performance

Wave Health is designed as a lightweight web application optimised for performance across varying network conditions. Specific performance SLAs are not contractually committed but are monitored internally.

7.3 Support Hours

Parameter	Detail
Standard Support Hours	Monday – Friday, 9:00 AM – 5:00 PM Pacific Time
Support Channel	Email
Target Response Time	1 business day

Note: UK/GMT timezone support hours are planned for future availability.

7.4 Emergency Escalation

For critical issues outside standard support hours, an emergency escalation path is available through the designated account contact.

8. Technical Requirements

8.1 Browser Support

Wave Health supports all major web browsers for the current and previous two major versions:

- Google Chrome
- Mozilla Firefox
- Apple Safari
- Microsoft Edge

8.2 Mobile Application

Platform	Minimum Version
Android	API Level 26 (Android 8.0)
iOS	iOS 16

8.3 Network Requirements

Wave Health is designed as a lightweight application with minimal bandwidth requirements. No specific firewall rules or IP whitelisting are required for standard operation.

8.4 Authentication

- Email and password authentication
- Multi-factor authentication (MFA) is **required** for all users

8.5 Accessibility

Wave Health has conducted an accessibility audit and is actively working to improve accessibility compliance. Formal WCAG certification is not currently available.

8.6 Integration (Planned)

The following integration capabilities are on the product roadmap:

Feature	Status
Single Sign-On (SSO/SAML)	Planned
API Access	Planned
HL7 FHIR Interoperability	Planned

9. Outage and Incident Management

9.1 Incident Classification

Incidents are classified by severity to ensure appropriate response:

Severity	Description	Example
Critical	Complete service unavailability	Platform outage affecting all users
High	Major feature unavailable	Core functionality impaired
Medium	Partial impact	Non-critical feature affected
Low	Minimal impact	Cosmetic issues, minor bugs

9.2 Customer Notification

Parameter	Commitment
-----------	------------

Notification Method	Email to designated contacts
Initial Notification	Within 4 hours of incident identification
Updates	Provided as material information becomes available
Resolution Notice	Sent upon incident closure

9.3 Post-Incident Review

Internal post-incident reviews are conducted for all Critical and High-severity incidents. Summary information may be provided to affected customers upon request.

10. Hosting and Data Residency

10.1 Regional Deployment

Wave Health operates dedicated infrastructure in multiple geographic regions to meet data residency requirements:

Customer Location	Hosting Region	Infrastructure
United States	AWS us-west-2 (Oregon)	Amazon Web Services
United Kingdom	AWS eu-west-2 (London)	Amazon Web Services
European Union	AWS eu-central-1 (Frankfurt)	Amazon Web Services
Serbia	OCI eu-jovanovac-1	Oracle Cloud Infrastructure

10.2 Region Assignment

Customers are assigned to a hosting region based on their jurisdictional and data residency requirements. Customers cannot self-select hosting regions, but will be deployed to a region that meets all applicable regulatory requirements.

10.3 Data Residency Guarantee

Patient health information (PHI) is stored and processed exclusively within the assigned hosting region. PHI is never transferred across regional boundaries.

10.4 Sub-Processors

The following third-party services are used to deliver Wave Health. None of these services processes personally identifiable information (PII) or protected health information (PHI):

Sub-Processor	Purpose	Data Processed
Google Analytics	Usage analytics	Anonymised usage metrics
CleverTap	User engagement analytics	Anonymised engagement data
New Relic	Performance monitoring	System telemetry (no PII)

Infrastructure providers (AWS, OCI) process PHI within the designated regional boundaries and are subject to appropriate data processing agreements.

11. Security

11.1 Certifications and Attestations

Certification	Status	Validity
ISO/IEC 27001:2022	In Progress	Expected Q1 2026
Cyber Essentials	Current	Renewed annually (April 2025)
HIPAA	Attestation	Current
UKCA Class I Medical Device	Registered	May 2025 (no expiry)

11.2 Encryption

Layer	Standard

Data at Rest	AES-256 encryption (AWS KMS-managed keys)
Data in Transit	TLS 1.2 or higher for all connections

11.3 Authentication and Access Control

- Email and password authentication for all users
- Multi-factor authentication (MFA) **required**
- Role-based access control (RBAC) for all platform functions

11.4 Security Testing

Activity	Frequency
Penetration Testing	Annual (third-party)
Vulnerability Scanning	Continuous

Penetration test summary reports are available to customers upon request, subject to an NDA.

11.5 Vulnerability Management

Identified vulnerabilities are remediated according to severity:

Severity	Remediation Target
Critical	7 days
High	30 days
Medium	90 days
Low	Best effort

11.6 Security Documentation

The following security documentation is available to customers and prospective customers upon request:

- Security questionnaire responses

- Penetration test summary (subject to NDA)
- Certification documentation

12. Regulatory Compliance

Wave Health is designed to support compliance with the following regulatory frameworks:

Regulation	Scope
HIPAA	United States healthcare privacy
GDPR	European Union data protection
UK GDPR	United Kingdom data protection
Serbian Data Protection Law	Republic of Serbia
NHS Data Security and Protection Toolkit	NHS England (where applicable)

Customers remain responsible for their own regulatory compliance obligations. Wave Health provides the technical and operational controls to support customer compliance programmes.